MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 3, 2015/2016

TNS3131 – NETWORK SECURITY AND MANAGEMENT

(All sections / Groups)

31 MAY 2016
9.00 a.m. – 11.00 a.m.
(2 hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 5 pages of **PART A with 20 multiple choice questions** and **PART B with 5 questions**.

2. Attempt **ALL questions in PART A** and **FOUR out of FIVE questions in PART B**. All questions carry equal marks and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

PART A – Multiple Choice Questions [20 marks]
Answer all questions.

1. _____ is the most common method used in digital signatures to conceal small blocks of data such as encryption keys and hash function values.

   A) Symmetric encryption
   B) Data integrity algorithms
   C) Asymmetric encryption
   D) Authentication protocols

2. A loss of _____ is the unauthorized disclosure of information.

   A) authenticity
   B) confidentiality
   C) reliability
   D) integrity

3. An original intelligible message fed into the algorithm as input is known as _____, while the coded message produced as output is called the _____ .

   A) decryption, encryption
   B) plaintext, ciphertext
   C) deciphering, enciphering
   D) cipher, plaintext

4. _____ attacks exploit the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

   A) Cryptanalytic
   B) Brute-force
   C) Block cipher
   D) Transposition

5. The vast majority of network-based symmetric cryptographic applications make use of _____ ciphers.

   A) linear
   B) stream
   C) permutation
   D) block

6. A ring is said to be _____ if it satisfies the condition ab = ba for all a, b in R.

   A) cyclic
   B) commutative
   C) abelian
   D) infinite

7. The _____ is when a small change in plaintext or key produces a large change in the ciphertext.

   A) avalanche effect
   B) message padding
   C) key expansion
   D) auxiliary exchange

8. The _____ algorithm will work against any block encryption cipher and does not depend on any particular property of DES.

   A) cipher block chaining
   B) meet-in-the-middle attack
   C) counter mode attack
   D) ciphertext stealing

Continued ....

9. The _____ and _____ block cipher modes of operation are used for authentication.

A) OFB, CTR
B) ECB, CBC
C) CFB, OFB
D) CBC, CFB

10. Feistel proposed that we can approximate the ideal block cipher by utilizing the concept of a _____ cipher, which is the execution of two or more simple ciphers in sequence in such a way that the final result or product is cryptographically stronger than any of the component ciphers.

A) linear
B) permutation
C) differential
D) product

11. The SSL Internet standard version is called _____ .

A) SSH
B) HTTP
C) SLP
D) TLS

12. The most complex part of SSL is the _____ .

A) SSL Record Protocol
B) Handshake Protocol
C) Change Cipher Spec Protocol
D) Alert Protocol

13. The _____ is used to convey SSL-related alerts to the peer entity.

A) Change Cipher Spec Protocol
B) Alert Protocol
C) SSL Record Protocol
D) Handshake Protocol

14. Phase _____ of the Handshake Protocol in SSL establishes security capabilities.

A) 4
B) 1
C) 2
D) 3

15. The _____ is the event or condition that determines when the payload is activated or delivered.

A) propagation phase
B) trigger
C) infection mechanism
D) execution

16. A(n) _____ virus is a form of virus explicitly designed to hide itself from detection by antivirus software.

A) encrypted
B) polymorphic
C) stealth
C) metamorphic

Continued ....

17. A _____ is an individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

A) sniffer
B) misfeasor
C) clandestine user
D) masquerader

18. A _____ is an individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

A) clandestine user
B) misfeasor
C) masquerader
D) mole

19. The most promising approach to improve password security is _____.

A) user education
B) a proactive password checker
C) computer generated passwords
D) a reactive password checking strategy

20. _____ can be an effective means of protecting a local system or network of systems from network based security threats while at the same time affording access to the outside world via wide area networks and the Internet.

A) VPNs
B) Proxys
C) Firewalls
D) SOCKS

Continued ....

PART B – Structured Questions [40 marks]
Answer four (4) out of five (5) questions.

QUESTION 1

a) Security threats can be further classified into passive and active attacks.
   i) Differentiate passive and active attack. [2 marks]
   ii) Provide **TWO (2)** examples for each type of attack respectively. [2 marks]

b) Consider a telephone switching system that routes calls through a switching network based on the telephone number requested by the caller. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance (low, medium, or high) of the requirement. [3 marks]

c) Indicate the attacks for each security mechanisms by placing (Y) in the table below. (Redraw the table in your answer script) [3 marks]

	Release of message contents	**Traffic analysis**	**Masquerade**	**Replay**	**Modification of messages**	**Denial of service**
Digital signature						
Access control						
Data integrity						
Authentication						
Routing control						
Notarization						

Continued ....

QUESTION 2

a) List any **FOUR (4)** essential ingredients of a symmetric cipher. [2 marks]

b) Briefly describe **THREE (3)** types of cryptanalytic attacks based on what is known to the attacker. [3 marks]

c) Public-key cryptography involves the use of two keys and the communication between sender and receiver is asymmetric. Explain the **TWO (2)** keys. [1 mark]

d) Given the parameters of RSA: p=19, q=11, e=7. Calculate the decryption key d. [4 marks]

QUESTION 3

a) Discuss **FOUR (4)** requirements for Kerberos. [4 marks]

b) List **FIVE (5)** types of S/MIME messages. [2.5 marks]

c) Illustrate the process of PGP message reception. [2 marks]

d) Give **THREE (3)** examples of applications of IPSec. [1.5 marks]

QUESTION 4

a) One type of threats on the web is confidentiality.
   i. Identify **TWO (2)** threats under confidentiality. [2 marks]
   ii. List a consequence of the confidentiality threat. [1 mark]
   iii. Define a countermeasure for the confidentiality threat. [1 mark]

b) Compare SNMPv1 with SNMPv2. List **TWO (2)** differences. [4 marks]

c) Explain **ONE (1)** strategy for selecting strong password. [2 marks]

QUESTION 5

a) One type of firewall is packet-filtering routers.
   i. Explain briefly the packet-filtering routers. [2 marks]
   ii. List **TWO (2)** advantages and **TWO (2)** disadvantages of the packet-filtering routers. [4 marks]

b) One of the threats in wireless network is eavesdropping.
   i. Define eavesdropping. [2 marks]

   ii. Explain **TWO (2)** methods to deal with eavesdropping. [2 marks]

End of Paper.